

# RFC-0013 SC-7 Boundary Protection Balance Improvement Release

---

## RFC Front Matter

- **Status:** Open
- **Created By:** FedRAMP
- **Start Date:** 2025-08-11
- **Closing Date:** 2025-09-11
- **Short Name:** rfc-0013-sc-7-boundary-protection

## Where to Comment

Members of the public may submit multiple different comments on different issues during the public comment period. The public is asked to please refrain from including documents or spreadsheets (especially those with in-line comments or suggested changes) in public comment as this creates a significant additional review burden.

Formal public comment for official consideration by FedRAMP can be made via the following mechanisms in order of preference:

1. GitHub Post: <https://github.com/FedRAMP/community/discussions/71>
2. Public Comment Form: <https://forms.gle/vgHHybwHwEe3Z6an7>
3. Email: [pete@fedramp.gov](mailto:pete@fedramp.gov) with the subject "**RFC-0013 Feedback**"

Note: FedRAMP will review and publicly post all public comments received via email, but will not otherwise respond. Email submissions from federal agencies will not be made public unless requested.

## Summary & Motivation

[FedRAMP does not plan to provide updated technical assistance](#) or guidance for implementations of the Rev5 baselines but [balancing Rev5 against improvements to FedRAMP 20x](#) remains important. SC-7 Boundary Protection requirements are currently imbalanced across these approaches: FedRAMP 20x Key Security Indicators encourage logical separation of network resources to prevent unwanted network traversal while Rev5 baselines limit network separation to Layer 3 subnetting as defined in IETF RFC-950.

To ensure consistency in a modern approach to boundary protection between FedRAMP 20x and Rev5, FedRAMP will begin an urgent Balance Improvement Release for Rev5 as follows:

1. On August 8, 2025, FedRAMP rescinded the “[Subnets White Paper](#)” to begin bringing Rev5 into balance with 20x by removing past guidance that prevented cloud service providers from using other technical capabilities that meet control SC-7.
2. FedRAMP will formalize updated SC-7 Boundary Protection guidance in all FedRAMP baselines to clarify how this control should be met for Rev5 authorizations. That proposed updated guidance is the primary content of this RFC.
3. When formalized after public comment, this Balance Improvement Release will **immediately** apply to all Rev5 baselines and authorizations. There will not be a separate beta period for this release. Stakeholders can expect this change to the Rev5 baselines to occur within 30 days of completing the public comment period.

## Effective Date(s) & Overall Applicability

This is a draft baseline update released for public comment; it does not apply to any FedRAMP authorization and MUST NOT be used in draft form.

- FedRAMP **20x**:
    - This baseline update clarifies underlying expectations for FedRAMP 20x controls but does not apply directly to FedRAMP 20x.
  - FedRAMP **Rev5**:
    - This baseline update will apply immediately to all Rev5 baselines and authorizations when formally released.
- 

## NIST SC-7 Boundary Protection Control Statement

The NIST SP 800-53 Rev5 contains the following text for the SC-7 Boundary Protection control:

- a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
- b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
- c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

# FedRAMP SC-7 Boundary Protection Control Expectations

The following updates will apply to all FedRAMP baselines under SC-7 Boundary Protection (current guidance or procedures will be entirely replaced with the updated guidance or procedures):

## SC-7 Control Requirement(s)

Current FedRAMP Guidance:

**SC-7 (b) Additional FedRAMP Requirements and Guidance:** SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper ([https://www.fedramp.gov/assets/resources/documents/FedRAMP\\_subnets\\_whitepaper.pdf](https://www.fedramp.gov/assets/resources/documents/FedRAMP_subnets_whitepaper.pdf)) for additional information.

Updated FedRAMP Guidance:

**SC-7 (b) Additional FedRAMP Requirements and Guidance:** SC-7 (b) may be met by using any technical capability that ensures logical separation between publicly accessible components and internal networks by preventing traversal without inspection and authorization; traffic may not flow unrestricted from publicly accessible components to internal networks.

## SC-7 Assessment Plan/Procedures

### Current Assessment Procedure:

Determine if:

- subnetworks for publicly accessible system components are physically; logically separated from internal organizational networks; and

### Updated Assessment Procedure:

Determine if:

- publicly accessible system components are logically separated from internal organizational network devices; and